Cryptography 1st Homework

3.13.20 Let a and $n > 1$ be integers with $\gcd(a, n) = 1$. The order of $a \mod n$ is the smallest positive integer r such that $a^r \equiv 1 \pmod{n}$. We denote $r = ord_n(a)$

a. Show that $r \leq \phi(n)$

b. Show that if $m = rk$ is a multiple of r, then $a^m \equiv 1 \pmod{n}$.

c. Suppose $a^t \equiv 1 \pmod{n}$. Write $t = qr + s$ with $0 \leq s < r$. Show that $a^s \equiv 1 \pmod{n}$.

d. Using definition of r and fact that $0 \leq s < r$, show $s = 0$, and therefore $r|t$. This, combined with part (b), yields the result that $a^t \equiv 1 \pmod{n}$ iff $ord_n(a)|t$.

e. Show that $ord_n(a)|\phi(n)$.